VO
Telekommunikation
389.057

Bakkalaureatsarbeit

Kryptographie

SS 2004
Demmelmayr Florian
0225642

Inhaltsverzeichnis

Einleitung

Die Kryptographie wurde erst in den letzten Jahren zu einer anerkannten Wissenschaft. In ihren Anfängen war man vor allem daran interessiert, während eines Krieges Nachrichten unbemerkt am Feind vorbeizuschmuggeln. Nachdem der Gegner einen Boten als solchen erkannt hatte, war es ihm ein Leichtes seine Meldung zu lesen und damit dem Sender in die Karten zu sehen.
Cäsar begann mit der Verschlüsselung seiner Befehle, damit der Feind mit ihnen nichts anfangen konnte.
Kryptographie und ihr natürlicher Feind, die Kryptoanalyse, entwickelten sich immer weiter, so dass auf der einen Seite immer bessere Codes gesucht wurden und andererseits immer neue Methoden sie zu knacken.
Mit der Industrialisierung kamen verstärkt maschinelle Chiffriergeräte zum Einsatz. Das wohl bekannteste war die deutsche Enigma, bei der sich die Alliierten vor und während des 2. Weltkrieges oft die Zähne ausbissen.
Wie so oft verhalf auch bei der Kryptographie das Militär der zivilen Welt zu einer wichtigen Erfindung. Die Enigma wurde immer komplizierter und so waren die Kryptoanalytiker gezwungen immer bessere Maschinen zu bauen, die die abgehörten Geheimtexte entschlüsseln konnten. So entstand der Colossus, ein Vorläufer des modernen Computers.
Im heutigen Informations- und Kommunikationszeitalter ist es immer wichtiger, auch Botschaften von normalen Menschen kryptographisch zu verändern, denke man z.B. an Geldtransfers oder Interneteinkäufe.

Die strenge Geheimhaltung kryptographischer und kryptoanalytischer Leistungen haben heute noch zur Folge, dass Verdienste herausragender Persönlichkeiten keine öffentliche Anerkennung finden. Erst im Laufe der letzten Jahrzehnte wurden immer mehr Taten aus früherer Zeit veröffentlicht, aber manche werden wohl nie ihre verdiente Würdigung finden.

1. Entstehung der Kryptographie

1.1 Von der Steganographie zur Kryptographie

Die Steganographie, abgeleitet von den griechischen Wörtern steganos (bedeckt) und graphei (schreiben) versucht mit dem Verbergen der eigentlichen Existenz einer Nachricht diese geheim zu halten.
Das wohl bekannteste Beispiel ist das Schreiben mit unsichtbarer Tinte, die der Empfänger durch Erhitzen sichtbar macht. Weiters in Verwendung sind Semagramme, sichtlich getarnte Geheimschriften, die eine Geheimnachricht in einer harmlos erscheinenden Umgebung verstecken. So werden verschiedene Buchstaben eines Textes, z.B. eines Zeitungsartikels, für Außenstehende fast unmerklich gekennzeichnet, der Empfänger erkennt diese und erhält dadurch den eigentlichen Text. Das Übermitteln von Botschaften als versteckte Morsecodes in Bildern ist ein ebenfalls typisches Beispiel für ein Semagramm.

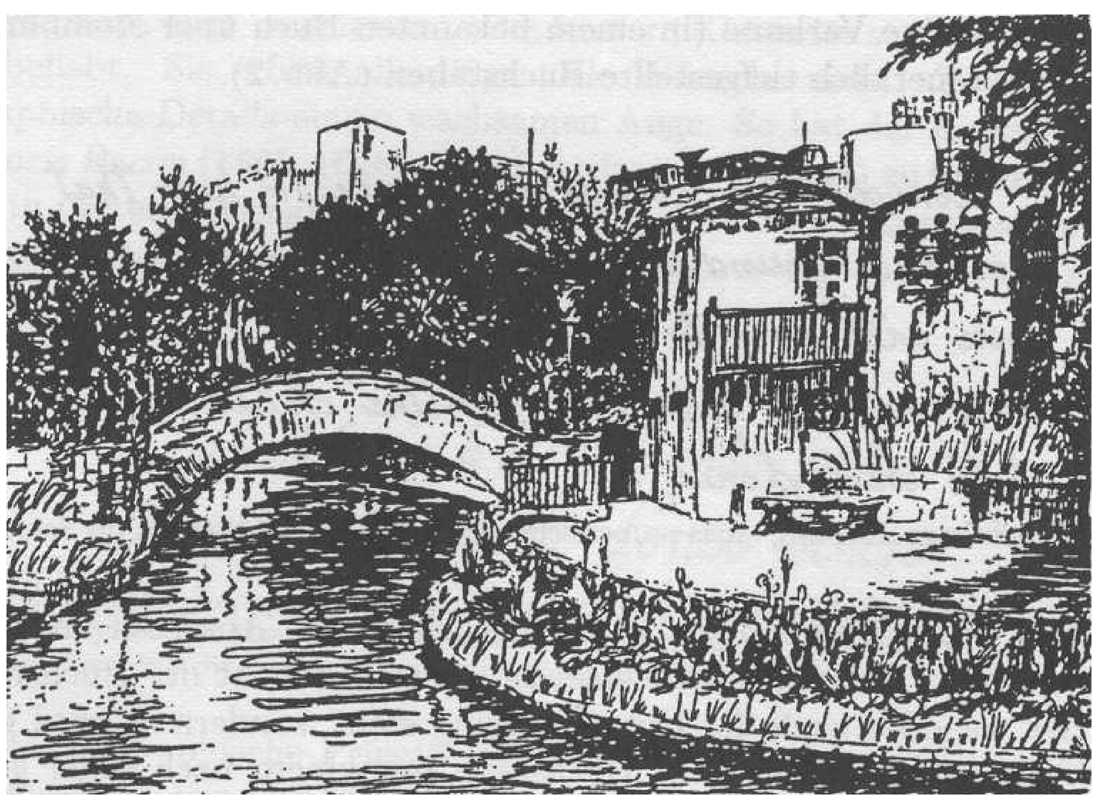


Abb.1:Semmagramm; Die Nachricht steht im Morsecode, der aus langen und kurzen Grashalmen, links von der Brücke, entlang des Baches und auf der kleinen Mauer abgebildet wird.

Die Grundidee der Steganographie ist, dass nur der, der weiß, dass etwas versteckt ist und wo es ist, es auch finden kann. Da dies ein gewisses Maß an Sicherheit bietet, hat sich die Steganographie sehr lange bewährt. In ihrem Prinzip liegt aber auch ihre größte Schwäche, denn hat man die Nachricht erst einmal gefunden, ist ihr Inhalt sofort erkenntlich.

Bei der Kryptographie, abgeleitet vom griechischen kryptos (verborgen) ist nicht das Verstecken einer Nachricht an sich, sondern das Verschleiern das Ziel. Dies geschieht mittels des Verfahrens der Verschlüsselung. Dabei wird durch eine vorher zwischen Sender und Empfänger vereinbarte Methode die Botschaft verändert. Mit dem so genannten Schlüssel ist es dem Empfänger dann möglich, die ursprüngliche Meldung zu rekonstruieren. Ein Gegner, der die Nachricht abfängt, kann mit dieser nur schwer etwas oder gar nichts anfangen, sofern er den Schlüssel nicht kennt.

1.2 Arten der Kryptographie

1.2.1 Transposition

Die Kryptographie stützt sich hauptsächlich auf die Transposition und die Substitution.
Bei der Transposition werden die Buchstaben einer Nachricht vertauscht, man erhält ein Anagramm. Bei einer großen Anzahl von Buchstaben wird die Anzahl der möglichen Anordnungen schnell sehr groß und es wird fast unmöglich, ohne Kenntnis des angewandten Umstellungsverfahrens die ursprüngliche Botschaft zu rekonstruieren. Eine einfache Form der Transposition ist die spartanische Skytale, ein Zylinder z.B. aus Holz, mit der die Generäle der Spartaner geheim miteinander kommunizierten.

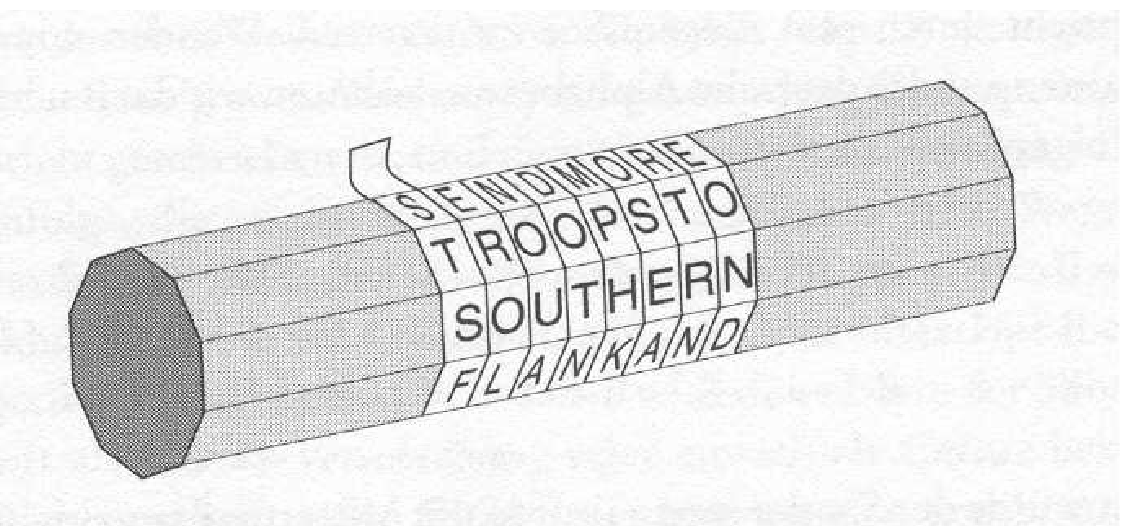


Abb.2: Spartanische Skytale

Der Sender wickelte ein Band um den Zylinder, oder ein Vieleck, und schrieb die Botschaft quer über das Band, anschließend wurde das abgewickelte Band dem Empfänger übermittelt. Dieser konnte mit einem Zylinder gleichen Durchmessers die Nachricht ohne Schwierigkeiten lesen.

1.2.2 Substitution

Bei der Substitution werden Buchstaben des Klartextes durch andere ersetzt. Da die heutige Kryptographie vermehrt auf die Substitution setzt, werde ich mich jetzt hauptsächlich mit diesem Verfahren beschäftigen.

2. Nichtmechanische Kryptographie in der Vergangenheit

2.1 Verschlüsselung nach Cäsar

Als Begründer der Kryptographie gilt C. J. Cäsar (100 - 44 v. Chr.).
Bei seinem Code benutzt man zwei Alphabete, das Klartextalphabet in natürlicher Reihenfolge und das Geheimtextalphabet, das darunter geschrieben wird und um ein paar Stellen verschoben ist.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Zum Verschlüsseln wird nun jeder Buchstabe der Botschaft durch den darunter stehenden des Geheimtextalphabetes ersetzt.
So wird G E H E I M zu J H K H L P.
Das Entschlüsseln ist ebenso einfach. Im 15. Jh. wurde dafür vom italienischen Architekten Leon Alberti eine kleine Maschine erfunden, mit der man das Ver- und Entschlüsseln automatisieren konnte.



Abb.3: Dechiffrierscheibe der Konföderierten

Diese Scheibe wurde im amerikanischen Bürgerkrieg eingesetzt. Sie beruht auf dem Mechanismus von Alberti. Den Geheimtext erhält man, wenn man von den beiden konzentrischen Kreisen von außen nach innen liest und umgekehrt den Klartext.

2.2 Schlüssel und Algorithmus

Ein kryptographisches Verfahren setzt sich zusammen aus einem Algorithmus und einem Schlüssel. Der Algorithmus ist die Vorschrift, wie aus einem Klartext ein Geheimtext gemacht werden kann. Beim Cäsar-Verfahren kann man sich diesen als Anwendung der vorher gezeigten Scheibe vorstellen. Der Schlüssel ist die Angabe, wie der Algorithmus nun konkret angewendet werden muss. Der Cäsar-Code besteht aus 26 Schlüssel, der Anzahl verschiedener Anordnungen der beiden Alphabete zueinander. Nur mit beiden Teilaspekten der Kryptographie kann ein Text einfach ver- und entschlüsselt werden. Das Ziel eines Gegners ist es nun, das eigentliche Geheimnis von Sender und Empfänger, den Schlüssel, zu knacken und damit die Botschaft brauchbar mitzuhören. Der Algorithmus ist normalerweise im Vergleich zum Schlüssel sehr komplex, man muss aber nach gewisser Zeit damit rechnen, dass ihn der Angreifer kennt. Ein Verfahren muss so gut sein, folgerte der niederländische Philologe Nieuwenhof (1835 – 1903) daraus, dass es durch Bekanntwerden des Systems nicht leidet. Wurde eine Cäsar-Maschine gefunden, wusste der Gegner nur die Art des Codierungsverfahrens, er kannte aber nicht den Schlüssel.

2.3 Kryptoanalyse des Cäsarcodes

2.3.1 Ausprobieren aller Möglichkeiten

Prinzipiell gibt es 2 Methoden den Cäsarcode zu knacken, entweder durch Ausprobieren aller Möglichkeiten oder durch statistische Analyse. Ersteres braucht beim Cäsarcode nicht sehr lange, da es nur 26 Möglichkeiten gibt (nur Buchstaben vorausgesetzt), die beiden Alphabete untereinander anzuordnen. Hat man einen sinnvollen Text gefunden, kann die Analyse beendet werden. Daher ist der Cäsarcode sehr unsicher.
Eine Verbesserung wird durch beliebige Anordnung des Geheimtextalphabetes erreicht, dadurch ergeben sich 26! mögliche Schlüssel. Es handelt sich auch dabei um ein monoalphabetisches Verfahren, da nur ein Geheimtextalphabet verwendet wird. Durch die sehr große Anzahl von Schlüsseln wird ein Ausprobieren aller Möglichkeiten nur mit speziellen Computern möglich sein.

2.3.2 Statistische Analyse

Für arabische Gelehrte waren die Jahre von 800 bis 1200 n. Chr. eine Epoche großartiger intellektueller Leistungen. Zu der Zeit, als Europa noch tief im Mittelalter steckte erfand der Gelehrte Al-Kindí die Kryptoanalyse. Er verfasste ein Werk mit dem Titel „Abhandlung über die Entzifferung kryptographischer Botschaften". Es enthält Untersuchungen über statistische Analyse von Geheimtexten.
In jeder lebenden Sprache kommen nicht alle Buchstaben gleich häufig verteilt vor. So gibt es z.B. im Deutschen sehr häufige, vorneweg das E, das fast ein Fünftel eines Textes ausmacht, gefolgt vom N. Im Gegensatz dazu kommen J, Q, X und Y eher selten vor. Führt man im Geheimtext eine statistische Analyse durch und verschiebt das Alphabet so, dass der häufigste Klartextbuchstabe beim häufigsten Geheimtextzeichen steht, oder man geht den umgekehrten Weg des seltensten, hat man schnell die Botschaft des einfachen Cäsarcodes entschlüsselt. Auch bei einer beliebigen Anordnung des Alphabetes führt die statistische Analyse zum Ziel. Man benutzt diesmal zusätzlich häufig aufeinander folgende Paare, wie EN, ER und CH, um dem Sender auf die Schliche zu kommen. So kann man schon sehr bald die meisten der möglichen Schlüssel ausschließen und schließlich durch Probieren die fehlenden Buchstaben einsetzen, um einen sinnvollen Text zu erhalten.

2.4 Die Überführung Maria Stuarts mittels der Kryptoanalyse

Die ehemalige schottische Königin und Katholikin Maria Stuart konnte am 8. Februar 1587 nur auf Grund der Werke eines Kryptoanalytikers hingerichtet werden. Katholische Edelleute wollten die protestantische, englische Königin Elisabeth I. ermorden lassen und an ihrer Stelle, ihre in Gefangenschaft befindliche Kusine Maria an die Macht bringen. Da der Austausch von Botschaften in das Gefängnis sehr gefährlich war, verwendete man ein eigenes Verschlüsselungsverfahren.

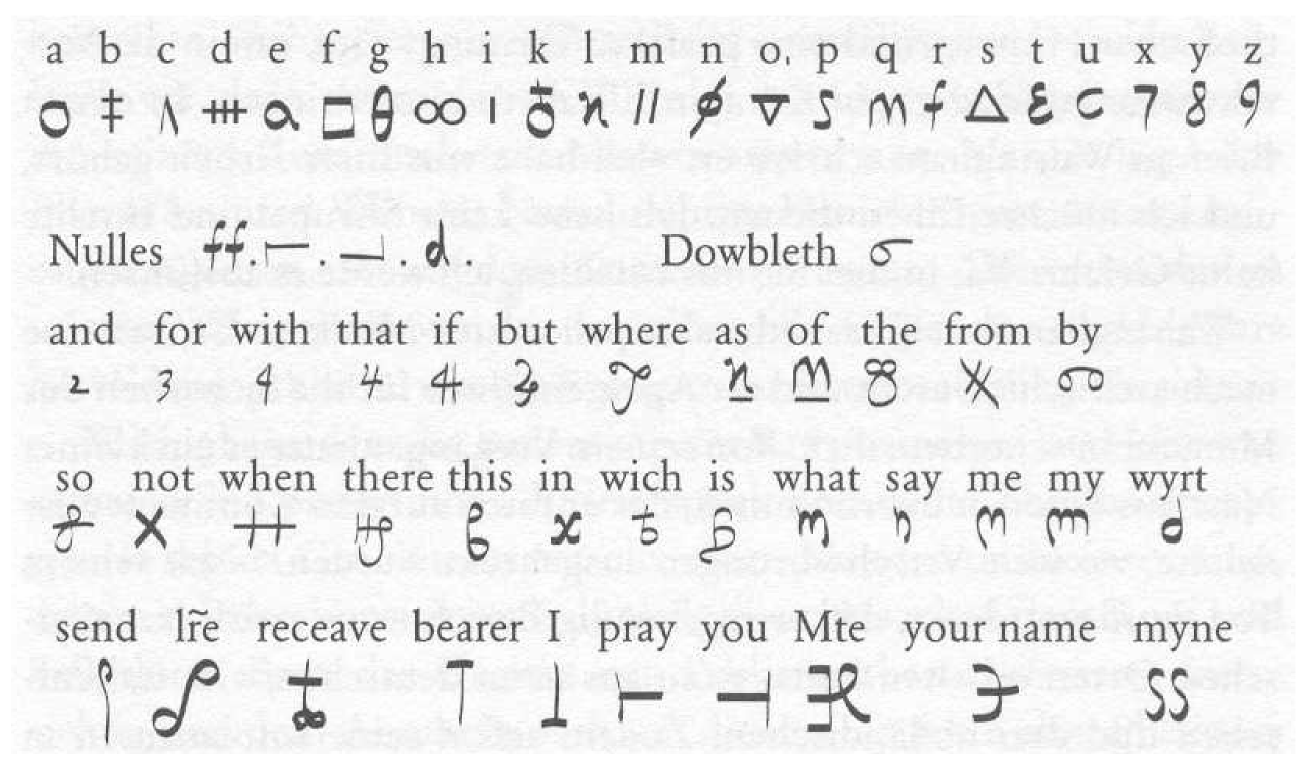


Abb.4: Schlüsselverzeichnis der Maria Stuart

Dem Kryptoanalytiker Thomas Phelippes, einem der besten Europas zu dieser Zeit, gelang es die Botschaften mittels Häufigkeitsanalyse zu entschlüsseln und schließlich Maria Stuart und die katholischen Edelleute zu überführen und dadurch ihre Hinzurichtung zu rechtfertigen.

2.5 Die Entwicklung der Polyalphabetischen Verschlüsselung

1587, also im selben Jahr der Hinrichtung Maria Stuarts, veröffentlichte Blaise de Vigenère seine Abhandlung von Geheimschriften.


Abb.5: Blaise de Vigenère

Sein Werk basiert auf der Verwendung von vielen verschiedenen Geheimtextalphabeten und wird deshalb auch Polyalphabetische Verschlüsselung genannt. Die Vigenère-Chiffrierung verwendet unterschiedliche Cäsar-Codes, die durch ein Schlüsselwort gesteuert werden. Die Verschiebung der

Alphabete wird zyklisch auf den gesamten Klartext angewendet. Das Schlüsselwort sei zum Beispiel H A U S, dann verwendet man der Reihe nach immer wieder folgende Geheimtextalphabete:

H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

Das Schlüsselwort steht senkrecht und bestimmt somit die Anzahl der Verschiebungen im Cäsar-Code. Je länger das Schlüsselwort ist, umso komplizierter wird die Entschlüsselung. Die ursprüngliche Häufigkeit des Klartextes geht verloren und es war lange Zeit nicht mehr möglich den Geheimtext mittels statistischer Analyse zu knacken. Trotz dieses herausragenden Vorteils spielte die polyalphabetische Verschlüsselung in den folgenden 2 Jahrhunderten kaum eine Rolle.

2.6 Die schwarzen Kammern

Am Beginn des 17. Jh. hatten alle europäischen Mächte ihre „schwarzen Kammern“, Nervenzentren, in denen Botschaften entschlüsselt wurden. Die „Geheime Kabinettskanzlei“ in Wien war die berühmteste und schlagkräftigste unter ihnen.
Nach einem genauen Zeitplan wurden Briefe an, bzw. von Botschaften geöffnet und abgeschrieben, um dann mit gefälschtem Siegel wieder weiter versendet zu werden. Anschließend waren die Kryptoanalytiker am Zug, die die Geheimtexte entschlüsselten.
Durch die zunehmende Anzahl und steigende Effizienz der schwarzen Kammern wurde die monoalphabetische Chiffrierung, trotz diverser Verbesserungen, schlussendlich doch durch die kompliziertere Vigenère- Verschlüsselung ersetzt.

2.7 Die Wiener Geheime Ziffernkanzlei

2.7.1 Geschichte

Nach französischem Vorbild wurde die „Wiener Geheime Ziffernkanzlei“ gegründet. Bis heute sind keine genauen Angaben über ihr Entstehungsjahr bekannt.
Unter Kaiserin Maria Theresia wurde sie ab 1763 als „Geheime Kabinetts Kanzlei“ bezeichnet. Erst im 19. Jahrhundert wurde die Bezeichnung „Geheime Ziffernkanzlei“ bzw. „Geheimes Ziffernkabinett“ üblich. Bevor sie dem k&k Kabinett eingegliedert wurde, war sie bis zum Jahre 1812 selbstständig.
In den 1750er Jahren wurde das „Geheime Ziffernkabinett“ durch Baron Koch neu organisiert und beschäftigte sich fortan auch mit der Ausbildung von neuen Kryptologen.
Unter Kaiser Joseph II. waren die Methoden der Entschlüsselung schon fast zu gut, sodass auf gesendete Botschaften immer neue Schlüssel angewendet wurden. Auch das konnte aber den Erfolg nicht stoppen. In den folgenden Jahren stieg die Anzahl der beschäftigten Beamten immer mehr an und die Kanzlei gewann immer mehr an Bedeutung. Entscheidender Anteil am Erfolg hing von der Zusammenarbeit mit der Post ab, daher wurde diese bestens forciert. Die Benutzung von Postämtern in der Umgebung von Wien war ein beliebter Weg sich der Beobachtung durch die „Geheimen Ziffernkanzlei“ zu entziehen, deshalb wurden die dortigen Postmeister beauftragt Briefe nicht direkt zuzustellen, sondern sie an das Hofpostamt in Wien zu senden.
Nach dem Tod Joseph II. verfiel die vorher so streng organisierte Kanzlei zusehends und führte nur noch zufällige Kontrollen im Inland durch. Die früher so gut gepflegten Beziehungen zu ausländischen Poststellen wurden rarer.

Erst Fürst Metternich nahm sich der Reorganisation der „Geheimen Ziffernkanzlei“ wieder an. In den Wintermonaten von 1814 auf 1815, während des Wiener Kongresses, wurde die Arbeit wieder intensiviert und die Polizeihofstelle gewann an Einfluss.
Nachdem während der Märzrevolution die Arbeit völlig eingestellt wurde, kam es noch einmal zu einer Neuorganisation.
Auf Druck der Presse und um den Kaiser nicht in Verlegenheit zu bringen, wurde die „Geheime Ziffernkanzlei“ am 4. April 1848 durch kaiserlichen Beschluss offiziell aufgelöst. Gleichzeitig wurde das Postpersonal für das Verletzen des Postgeheimnisses verantwortlich gemacht.

2.7.2 Tätigkeit

Die Arbeiten der „Geheimen Ziffernkanzlei“ waren streng organisiert. Gewöhnlich trafen die ersten Posttaschen der nach Wien eingehenden Briefe um 7 Uhr früh ein. Die Beamten untersuchten die Sendungen und gaben die interessant scheinenden Briefe an Kollegen weiter. Dann wurde entweder ein Abdruck des Siegels gefertigt, oder aber das verwendete Siegel befand sich bereits im Siegelkasten der Kanzlei. Botschaften von Interesse wurden kopiert und bei Bedarf ins Deutsche übersetzt. Nach dem Schließen der Briefe wurden nochmals die Siegel überprüft und die Briefe wurden um halb 10 wieder an die Post geschickt.
Um 10 Uhr kamen dann die Briefe an, die durch Wien gesendet wurden. Für diese Briefe konnte man sich etwas mehr Zeit lassen.
Die Polizeihofstelle schickte von ihr abgefangenen Sendungen von Flüchtlingen und politischen Gefangenen gegen 11 Uhr.
Am Nachmittag, um 16 Uhr kamen von Wien weggeschickte Briefe in die „Geheime Ziffernkanzlei“.
Ein Grundsatz der Kanzlei war es, den normalen Postbetrieb auf keinen Fall zu lange aufzuhalten. Im Notfall arbeiteten an einer Kopie vier Personen, wobei zwei den anderen diktierten.
Die entzifferten, übersetzten und abgeschriebenen Briefe kamen alle zum Kanzleidirektor. Mit Umwegen über die Polizeihofstelle wurden die Kopien zum Kaiser weitergeleitet. Nachdem auch der Staatskanzler die Möglichkeit hatte sie einzusehen, sendete man sie an das „Geheime Ziffernkabinett“ zurück und vernichtete sie dort nach etwaiger Lagerung.
Täglich wurden so ca. 80 bis 100 Sendungen behandelt.

2.7.3 Personal

Die geheime Ziffernkanzlei war vergleichbaren Organisationen im Dechiffrieren geheimer Botschaften weit voraus. Kaiser Karl VI ließ es sich daher nicht nehmen, jedem Dechiffrierer sein Gehalt persönlich auszuzahlen. In die Arbeit der Kanzlei brachte sich auch Kaiserin Maria Theresia ein, die oft mit Beamten diskutierte oder die Verwendung neuer Schlüssel für die eigene Post anordnete.
An die Angestellten der geheimen Ziffernkanzlei wurden hohe Anforderungen gestellt, vor allem aber mussten sie einen Eid auf Treue zum Vaterland und auf strengste Geheimhaltung leisten. Um aufgenommen zu werden, musste man diverse Fremdsprachen sprechen und auch in Algebra und elementarer Mathematik geübt sein. Vor der Einstellung folgte eine weitreichende Ausbildung im Dechiffrieren.

2.8 Die Dechiffrierung der Vigenère- Verschlüsselung

Charles Babbage, geboren 1791 in London, war einer der besten Kryptoanalytiker des 19.Jahrhunderts. Ihm gelang 1854 die Dechiffrierung der Vigenère- Verschlüsselung.

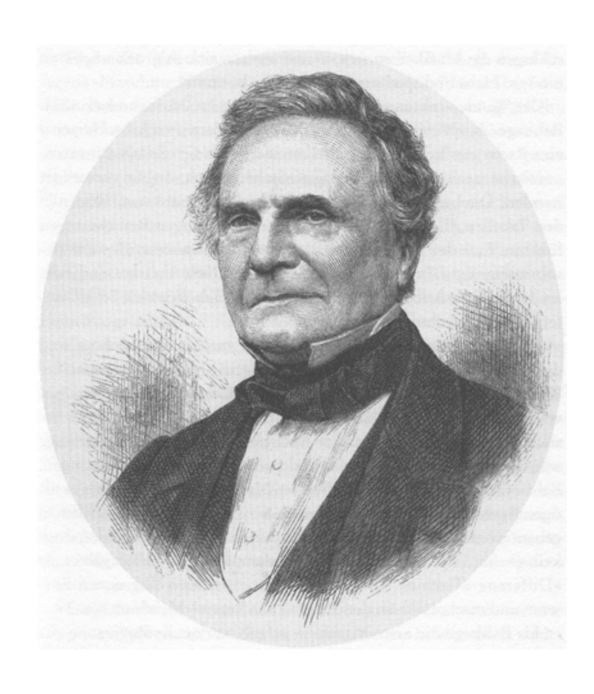


Abb.6: Charles Babbage

Unter anderem zählen die ersten Entwürfe eines modernen Computers zu seinen Verdiensten, dieser hatte bereits eine „Mühle“ (heute besser bekannt als Prozessor) und einen Speicher. Er war programmierbar und konnte verschiedenste Berechnungen durchführen. Leider konnte er aber nach einem ersten Fehlversuch auf Grund von Geldmangel nicht verwirklicht werden.

Ein Zahnarzt aus Bristol wollte 1854 eine Chiffrierung zum Patent anmelden, die der Vigenère-Verschlüsselung entsprach. Als Babbage das Patentamt darauf hinwies, dass es diese schon mehrere Jahrhunderte gebe, forderte ihn der Zahnarzt heraus, den Code zu knacken.
Babbage fand heraus, dass bei dieser Art der polyalphabetischen Verschlüsselung oft vorkommende Wörter gleich chiffriert werden. Durch die Abstände dieser gleichen Geheimtextwörter kann man bei einem längeren Text auf die Länge des Schlüsselwortes schließen. Weiß man, aus wie vielen Buchstaben der Schlüssel besteht, z.B. aus 5, so wendet man auf jeden 5. Buchstaben die bereits bekannte Häufigkeitsanalyse an. Bei diesem Beispiel wird jeder 5. Buchstabe des Klartextes mit dem selben Alphabet verschlüsselt und man erhält 5 monoalphabetische Chiffrierungen. Das als unbezwingbar gegoltene Vigenère- Verfahren war geknackt.
Für seinen Verdienst wurde Charles Babbage zu Lebzeiten nie gewürdigt, da seine Aufzeichnungen erst im 20. Jh. ans Licht kamen und unabhängig von ihm 1863 der pensionierte preußische Offizier Friedrich Wilhelm Kasiski die gleiche Methode entdeckte.

2.9 Kryptoanalyse während des 1. Weltkrieges

Ende des 19.Jh. hatten die Kryptographen keinen Code mehr zur Verfügung, der sicher war. Zusätzlich zu dieser Misere begann der italienische Physiker Guglielmo Marconi 1894 mit der Erforschung der Informationsübertragung mittels elektromagnetischer Wellen. Auf Grund dieser bahnbrechenden Erfindung war es dem Gegner möglich, die Nachrichtenübermittlung leicht mitzuhören. So wurden während des 1.Weltkrieges schätzungsweise hundert Millionen Wörter der Deutschen von den Franzosen mitgehört. Umgekehrt forcierten die Deutschen erst 1916, also nach 2 Kriegsjahren, ihre Kryptoanalyse-Abteilungen.
Durch das erfolgreiche Dechiffrieren eines Telegramms des deutschen Außenministers Arthur Zimmermann durch die Engländer wurde der Kriegsverlauf stark beeinflusst. Zimmermann teilte seinem Botschafter in Amerika mit, dass Deutschland den uneingeschränkten U-Bootkrieg beginnen wolle. Sollten sich die bis dahin neutralen Amerikaner daraufhin auf Seiten der Alliierten stellen, müsste Mexiko Amerika angreifen. So könne Deutschland in Europa ungehindert den Krieg weiter führen.

Nachdem die Engländer am ersten Kriegstag bereits das deutsche Transatlantikkabel gekappt hatten, mussten die Deutschen auf Funkverkehr und andere Leitungen ausweichen, die aber abgehört wurden. So wurde der wesentliche Sinn des Zimmermann Telegramms schon innerhalb eines Tages von der englischen „Schwarzen Kammer“, dem Room 40 dechiffriert, um später dann dem amerikanischen Präsidenten Wilson präsentiert zu werden. Um den Dechiffriererfolg geheim zu halten, stahl man das weitergeleitete, von der deutschen Botschaft in den USA entschlüsselte Telegramm in Mexiko und macht so Mexiko für das Bekanntwerden des Inhalts verantwortlich. Amerika stieg nach Beginn des U-Bootkrieges und der Gewissheit, die man durch das Telegramm erhalten hatte, ohnehin in den Krieg verwickelt zu werden, am 6. April 1917 in den Krieg ein.

2.10 Der unknackbare Code

Ende des 1. Weltkrieges erfanden amerikanische Wissenschafter eine neue Chiffriermethode. Statt wie bei der Vigenère- Verschlüsselung einfache Schlüssel zu verwenden, nimmt man welche, die gleich lang wie der Klartextes sind und aus Zufallsfolgen von Buchstaben bestehen. Das Zyklische an der Vigenère- Chiffrierung geht verloren und es ist dem Angreifer nicht möglich ohne Schlüssel den Code zu knacken. Die Schlüssel auf Zetteln bekommen Sender und Empfänger, die diese nach einmaligem Gebrauch vernichten, deshalb auch der Name One time pad.
Dieser bis heute als unbezwingbar geltende Code wird in der Praxis fast nie verwendet. Das hat zwei Gründe:
Um mehrere längere Botschaften zu verschlüsseln braucht man sehr viele One time pads und viel Zeit. Zwischen Sender und Empfänger muss eine ständige Verteilung stattfinden und die Synchronisation muss gewährleistet sein.
Der zweite Grund ist die sehr teuer herzustellende Menge an Zufallsbuchstaben. Das Wichtige ist die tatsächliche Zufälligkeit, die man z.B. durch die Auswertung radioaktiven Zerfalls erhalten kann. Aus diesen Gründen hat sich dieses Verschlüsselungsverfahren nie durchgesetzt.

3. Maschinelle Kryptographie

3.1 Die Enigma



Abb. 7: Wehrmachtsenigma mit 3 Rotoren

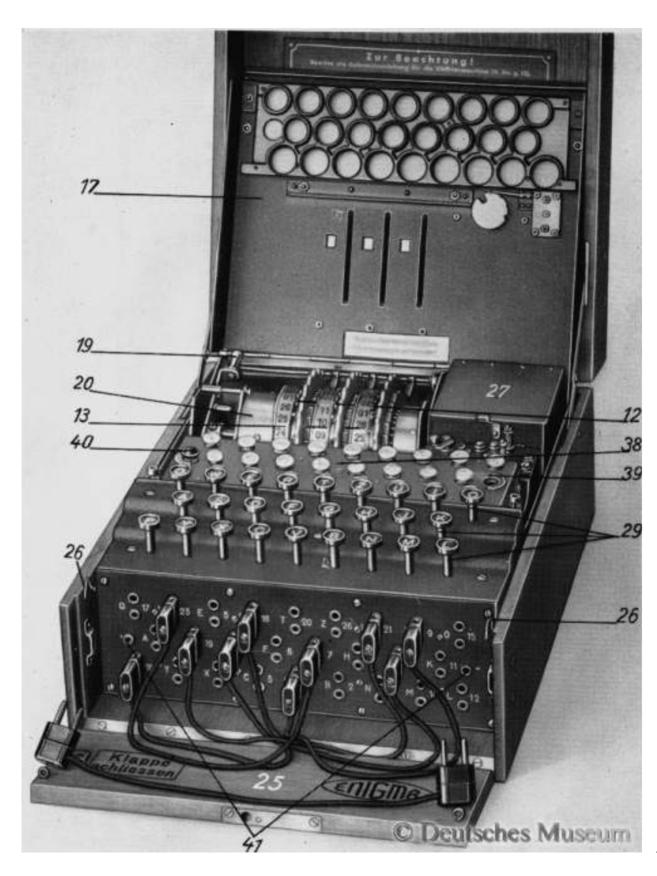
Seit der Erfindung der Chiffrierscheibe durch Alberti versuchte man immer neue Methoden der maschinellen Verschlüsselung zu erhalten. Die bekannteste Erfindung gelang dem deutschen Arthur Scherbius. Seine Enigma (griechisch: Rätsel) wurde zur gefürchtetsten Chiffriermaschine der Geschichte. Seine erstes Modell ließ er 1918 patentieren.



Abb. 8: Arthur Scherbius

3.1.1 Aufbau und Anwendung

Von außen sieht die Enigma aus wie eine altmodische Schreibmaschine. Durch einen Tastendruck wird Strom durch die Verschlüsselungseinheit geschickt, woraufhin ein Lämpchen aufleuchtet, das einen Buchstaben anzeigt. Ihr wahres Geheimnis liegt im Inneren.



12 Chiffrierwalzen
13 Zahlenringe
17 Metalldeckel
19 Haltehebel
20 Umkehrwalze
25 Stirnwand
26 Haken
27 Batteriekasten
29 Tastenbolzen
38 Glühlampenfeld
39 Lampenprüfung
40 Kabelprüfung
41 Unverw. Buchsen zur Kabelprüfung

Abb. 9: Zeichenerklärung der Enigmabestandteile

Sie besteht unter anderem je nach Modell aus drei bis fünf Rotoren, auch Walzen genannt, die im Inneren verdrahtet sind und so für sich allein, im Stillstand eine einfache monoalphabetische Verschlüsselung bewirken. Die Rotoren sind miteinander gekoppelt, ähnlich einem heute üblichen Kilometerzähler beim Auto. Nach jedem Tastendruck bewegt sich die erste Walze. Erst wenn sie sich einmal um ihre eigene Achse gedreht hat, bewegt sich die zweite um eine Position weiter. Da ein Rotor 26 Stellungen hat, für jeden Buchstaben einen, gibt es bei der Enigma mit drei Rotoren erst nach 26*26*26 Schritten wieder eine Wiederholung.







Abb. 10: Rotor der Enigma

Am Ende befindet sich der Reflektor, der das Stromsignal spiegelt und auf einem anderen Weg wieder durch die Walzen schickt. Schließlich gelangt der Strom zur Anzeige und ein Lämpchen leuchtet.

Damit man die Anzahl der möglichen Schlüssel der dreirotorigen Enigma von 17576 noch steigern kann, sind die Walzen vertauschbar, bei drei erhöht sich die Zahl der Möglichkeiten um den Faktor 3! also 6.

Um es dem Gegner noch schwieriger zu machen den Code zu knacken, entwickelte Scherbius ein Steckbrett an der Vorderseite seiner Maschine, das es ermöglichte zwei Buchstaben untereinander zu vertauschen. Bei 6 Vertauschungen und 26 Stellen multipliziert sich die Zahl der Schlüssel noch mit dem riesigen Faktor 100391791500. Die Gesamtmenge an Möglichkeiten, die Enigma einzustellen, lag bereits bei diesem frühen Modell um zehn Billiarden (10^{16}).

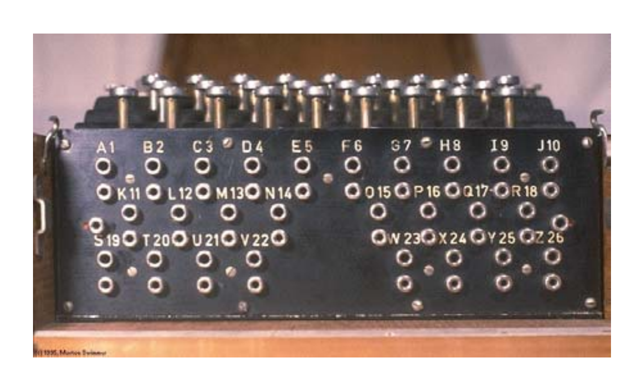


Abb. 11: Enigma Steckbrett

Der Empfänger stellte zu Beginn der Übertragung die Enigma auf den Schlüssel ein. Durch die Umlenkung durch den Reflektor im Inneren konnte er dann den empfangenen Geheimtext einfach in seine Maschine eingeben und sah auf der Anzeige die Buchstaben des Klartextes aufleuchten.
Trotz der enormen Sicherheit, die die Enigma bot, konnte Scherbius seine Erfindung anfangs nicht an den Mann bringen. Die Deutsche Armee war sich nicht bewusst, dass das Zimmermann-Telegramm dechiffriert wurde und für die Privatindustrie war die Maschine zu teuer. Winston Churchill veröffentlichte 1923 ein Buch, in dem er schilderte, wie die Engländer deutsche Botschaften während des ersten Weltkrieges abgefangen und dechiffriert hatten. So kam das deutsche Heer zur Überzeugung, dass Handlungsbedarf bestünde und Scherbius begann 1925 mit der Serienfertigung der Enigma. Insgesamt wurden über 30.000 Stück verkauft, obwohl Scherbius wegen seines Todes 1929 seinen Erfolg nicht mehr auskosten konnte.

3.1.2 Die Entschlüsselung der Enigma

Die Franzosen hörten nach Ende des Ersten Weltkrieges nach wie vor deutsche Funksprüche ab und entschlüsselten sie, aber ab 1926 stießen sie auf ein Rätsel. Sie konnten mit den von der Enigma chiffrierten Nachrichten nichts anfangen und da sie keine Bedrohung durch den Gegner mehr sahen, gaben sie auf. Im Gegensatz zu ihnen hatten die Polen Angst, die Deutschen könnten sich die an ihnen verlorenen Gebiete zurückerobern. So setzten sie alles daran die Enigma zu entschlüsseln.
Durch einen deutschen Spion, beschäftigt in der Berliner Chiffrierstelle, der Schaltzentrale der Enigma, gelangten die Polen zur „Schlüsselanleitung für die Chiffriermaschine Enigma“ und die „Gebrauchsanweisung der Chiffriermaschine Enigma“. Damit war die Dechiffrierung keineswegs möglich, da man noch immer nicht die Schlüssel kannte.

Der polnische Kryptograph Marian Rejewski beschäftigte sich mit der Analyse der Enigma.



Abb. 12 Marian Rejewski

Er erkannte, dass man die Walzenstellungen und deren Lagen vom Problem der Steckverbindungen trennen konnte. Damit gelang ihm der entscheidende Durchbruch.

Die Benutzer der Enigma hatten präzise Anordnungen wie sie ihre Arbeit zu tätigen hatten. Jeden Tag wurde ein neuer Schlüssel benutzt.
Beispiel für einen Tagesschlüssel:
(1) Steckverbindungen: A/L - P/R - T/D - B/W - K/F - O/Y
(2) Walzenlage: 2 - 3 - 1
(3) Grundstellung der Walzen: Q - C - W
Da sehr viele Meldungen verschickt wurden, gebrauchte man für jede Nachricht einen eigenen, selbst konstruierten Schlüssel, den der Sender dem Empfänger am Anfang der Meldung übermitteln musste. Dieser unterschied sich aber nur von der Grundstellung der Walzen zu beginn vom Tagesschlüssel. Um eine sichere Übertragung zu gewährleisten wurde er zweimal hintereinander gesendet. Wenn z.B. PGH der Schlüssel war wurde PGHPGH eingetippt und die Enigma lieferte z.B. KIVBJE.
Da man wusste, dass bei jeder Meldung am Anfang zwei Buchstaben vom selben Klartextbuchstaben stammen, konnten die Kryptoanalytiker Schlussfolgerungen über die Walzenstellungen tätigen.
Die von Rejewski entwickelte Maschine, genannt „Bombe“, konnte innerhalb von zwei Stunden die Grundstellung der Walzen ermitteln. Da sechs Walzenlagen möglich waren, ließ Rejewski auch sechs Bomben parallel laufen. Die gefürchtet Enigma war 1932 von den Polen bezwungen worden.

Deutsche Kryptographen verkomplizierten im Dezember 1938 die Scherbius-Maschine um eine Stufe. Es wurden zwei neue Walzen ausgegeben und so erhöhte sich die Möglichkeit der Walzenstellungen von sechs auf 60. Die Verkabelungen wurden auf zehn erweitert. Rejewski hätte 60 „Bomben“ gebraucht und war damit 1939 mit seiner Kryptoanalyse am Ende. Nachdem Hitler am 27. April 1939 mit Polen den Nichtangriffspakt aufkündigte, übergab man im August zwei Enigmanachbauten sowie je eine „Bombe“ an England und Frankreich. Zwei Wochen später, am 1. September fielen Hitlers Nationalsozialisten in Polen ein und der Krieg begann.

Durch die Erkenntnis der Bezwingbarkeit der deutschen Verschlüsselungsmaschine bekamen die Engländer neue Motivation. Man zog vom zu klein gewordenen Room 40 nach Bletchley Park, wo unter dem Mathematiker Alan Turing den Codeknackern immer neue Erfolge gelangen. Mit großem technischen Aufwand und mit der Kenntnis von Bedienungsfehlern gelangte man immer zu neuen Lösungsmethoden.

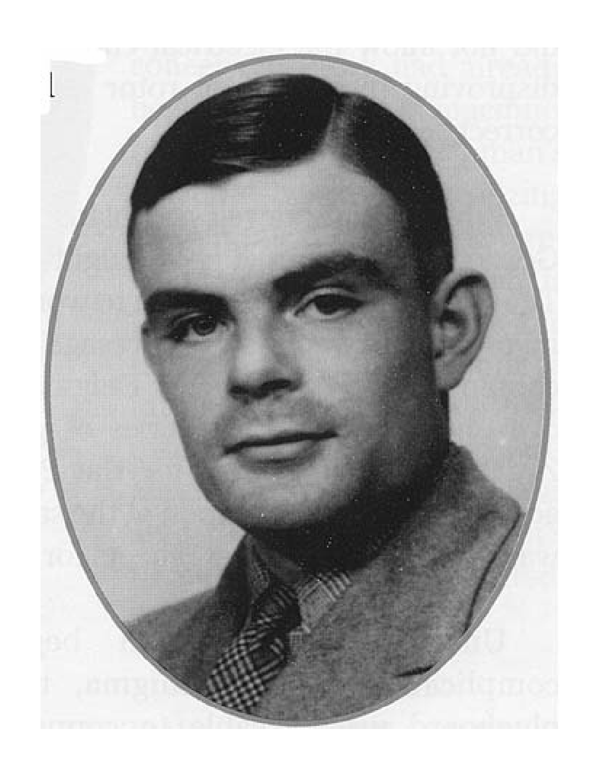


Abb. 13: Alan Turing

Die offensichtlichsten Anwendungsfehler lagen in der Zusammenstellung der Schlüssel. Eine Walze durfte nicht an zwei aufeinander folgenden Tagen an der selben Position stehen. Am Steckbrett musste man Buchstaben vertauschen, die im Alphabet nicht aufeinander folgten. Klingt eigentlich sinnvoll, nur wurde mit solchen Vorschriften die Zahl der Möglichkeiten drastisch reduziert. Auch waren die Funksprüche oft standardisiert, so wurde jeden Morgen zur selben Zeit das Wetter gefunkt und wer die Militärsprache kennt, weiß, dass sich diese nach einem genauen Muster verhält.
Man setzte in Bletchley Park eine Vielzahl von „Bomben" ein und entwickelte sie weiter. Die so genannte „Agnes" war viel schneller und konnte eine Vielzahl von Berechnungen durchführen.

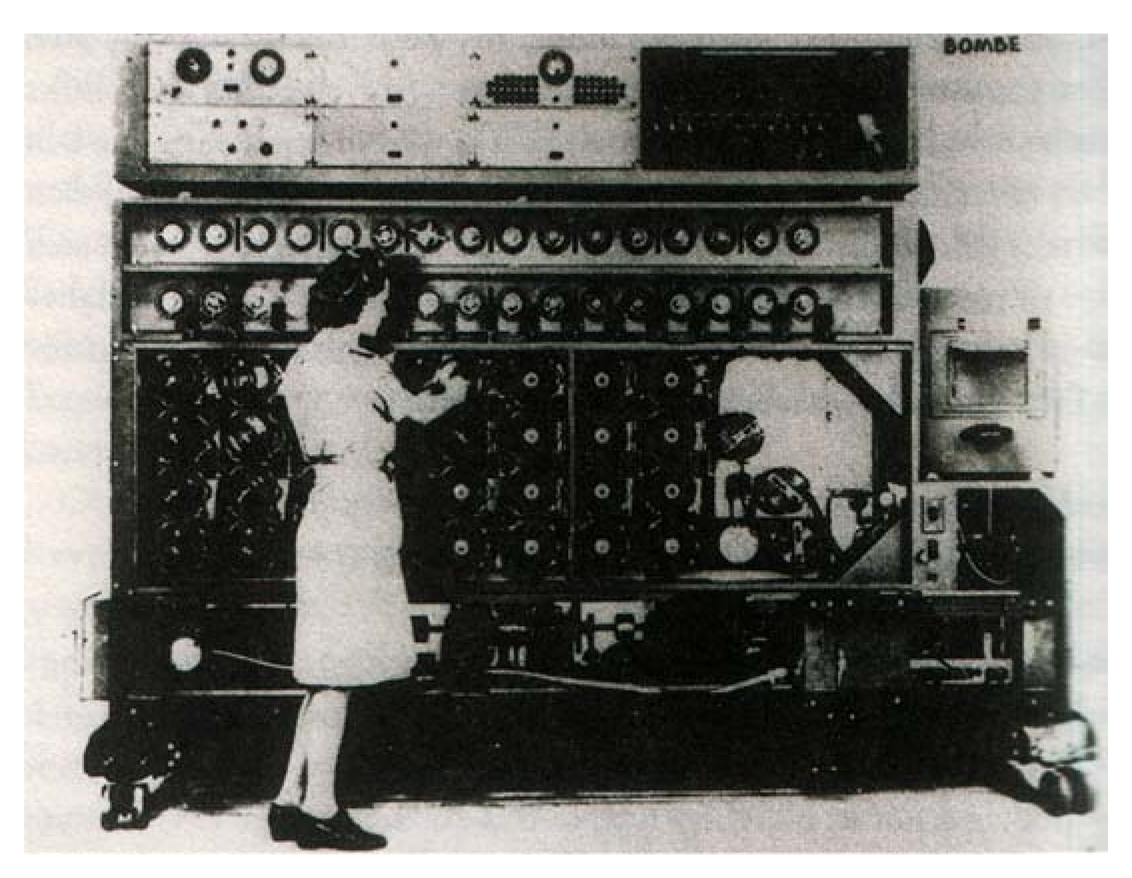


Abb. 14: Bombe in Bletchley Park
Eine große Kunst lag in der Geheimhaltung der Entschlüsselung. Die Engländer versenkten nicht alle Schiffe der Deutschen, deren Position sie kannten oder versuchten, dass ihre Siege nicht allzu glatt verliefen, nur um keinen Verdacht zu erregen. So wurde durch die geniale Arbeit der Kryptoanalytiker der Krieg verkürzt und viele Menschenleben gerettet.

3.2 Amerikanische Kryptographie während des 2. Weltkrieges

Während des Pazifikkrieges gelang den Amerikanern die Entschlüsselung der japanischen Purple-Maschine. Das Kräfteverhältnis wurde durch diesen Erfolg entscheidend beeinflusst.
Da man sich im schnell geführten Krieg nicht auf langsame Verschlüsselungsverfahren verlassen wollte, suchte man neue, schnellere Wege. Die amerikanische Kriegsmarine setzte für ihren Funkverkehr Ureinwohner vom Stamm der Navajos ein. Ihre Sprache war von dem europäischen und asiatischen Sprachen sehr verschieden und konnte unter anderem deshalb vom Feind nie entschlüsselt werden.

4. Kryptographie mittels Computer

4.1 Vorläufer des modernen Computers

Die in Bletchley Park eingesetzten „Bomben“ hatten einen großen Nachteil, sie waren nicht programmierbar. Um dieses Problem zu lösen baute man den Colossus, den Vorläufer des modernen digitalen Computers. Er bestand aus 1500 elektronischen Röhren und wurde am 8. Dezember 1943 nach Bletchley Park gebracht.

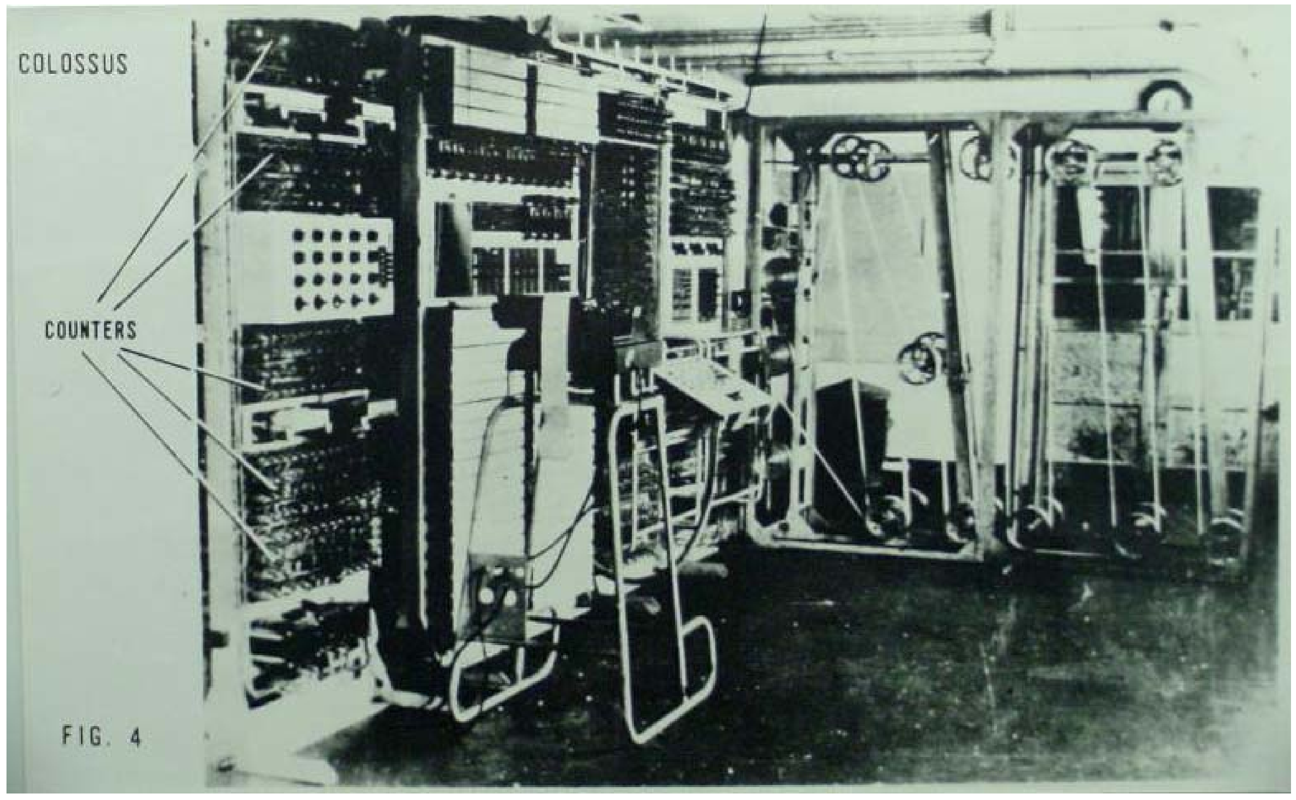


Abb.15: Colossus

Nach Kriegsende wurden alle Hinweise der englischen Kryptoanalyse vernichtet und so gelangte die amerikanische ENIAC (Electroinic Numerical Integrator And Calculator) 1945 zum Ruhm des

ersten Computers der Welt. Mit der zunehmenden Computerisierung kam man immer mehr von mechanischen Chiffriergeräten ab und suchte standardisierte computergesteuerte Verfahren.

4.1 Der DES

Der Data Encryption Standard, kurz DES, ist heute der populärste Verschlüsselungsalgorithmus. Er baut auf der von IBM entwickelten Methode „Lucifer“ auf, die schließlich von der National Security Agency (NSA) spezifiziert und 1976 standardisiert wurde.
Der DES verschlüsselt jeweils Blöcke mit 64 Bits auf einem Schlag mittels einem Schlüssel von 56 Bits. In Computern werden Daten als Folge von Bits gespeichert. Bei der Übertragung von Geheimtextbotschaften werden diese geblockt und mittels DES chiffriert.
Der Algorithmus ist keineswegs geheim, geschweige denn unknackbar, aber er ist sehr gut. Die Anzahl der möglichen Schlüssel beträgt 2^{56}, also über 72 Billiarden. Mit einem normalen Computer ist es nicht möglich diesen in ansprechender Zeit zu knacken. Um die Sicherheit zu erhöhen verwendet man zwei Schlüssel mit dem Triple-DES Verfahren. Der Klartext wird zuerst mit dem ersten Schlüssel und dann mit dem zweiten verschlüsselt. Zum Schluss wird der Text vor der Übertragung mit dem ersten Schlüssel wieder entschlüsselt. Die Zahl der möglichen Schlüssel erhöht sich demnach auf 2^{112}.

Die populärste Anwendung des DES Verfahrens ist der Bankomat. Die große Menge an Bankkunden und deren Geheimzahlen weltweit in riesigen Datenbanken zu speichern wäre unpraktikabel, deshalb steht der Code verschlüsselt auf dem Magnetstreifen der Karte. Ohne den zugehörigen Schlüssel hat niemand eine Change aus den gespeicherten Daten wie Bankleitzahl, Kontonummer, usw. die entsprechenden Geheimzahlen zu berechnen.
Am Beginn einer Bankomataktion berechnet der Apparat mittels der DES Entschlüsselung den PIN und vergleicht ihn mit der Eingabe des Kunden. Bei Gleichheit wird Geld ausgegeben und bei einer Differenz wird der so genannte Fehlbedienungszähler um eins erniedrigt.

4.3 Schlüsselverteilung

Mittels des DES ist es möglich Daten sicher zu übertragen, aber sowohl Sender als auch Empfänger müssen den selben Schlüssel benutzen. Das Problem ist die sichere Übermittlung der Schlüssel, dessen Beseitigung als größte kryptographische Leistung des 20. Jahrhunderts gilt. Bis dahin galt es als unmöglich, dass Personen ohne vorherige Schlüsselverteilung sicher Geheimnisse austauschen.

Die Amerikaner Whitfield Diffie und Martin Hellman beschäftigten sich mit der entscheidenden Frage: Kann ich jemandem, mit dem ich noch nie Kontakt hatte, insbesondere noch nie ein Geheimnis ausgetauscht habe, eine verschlüsselte Nachricht schicken, die nur er entschlüsseln kann? Sie beantworteten sie mit ja und führten die Lösung auf die Verwendung von mathematischen Einwegfunktionen zurück. Diese liefern in eine Richtung gerechnet einfach ein Ergebnis, in die andere aber nicht.

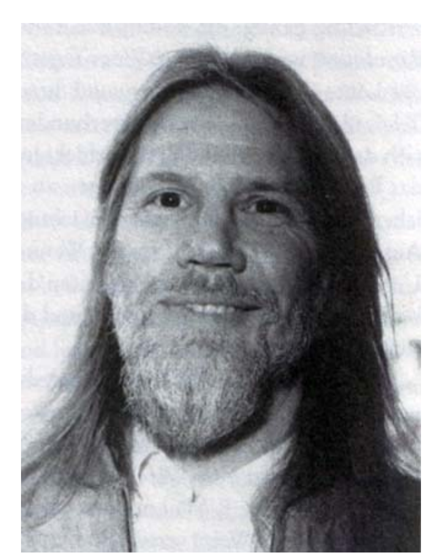
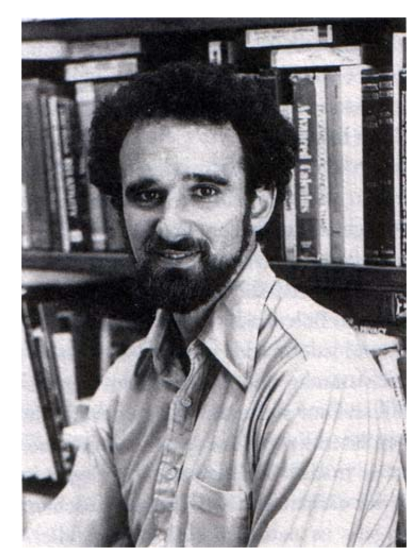



Abb. 16: links: Whitfield Diffie, rechts: Martin Hellman

Der Diffie-Hellman-Schlüsselaustausch ist wie folgt erklärt:
Sender und Empfänger einigen sich auf eine Primzahl p und eine natürliche Zahl s, für die gilt: $1 < s < p$, diese beiden Zahlen darf jeder Außenstehende wissen. Nun beginnt der zweistufige Prozess: Die Partner A und B wählen jeweils eine geheime Zahl a bzw. $b < p$ und potenzieren s mit ihnen, modulo p.
A berechnet: $\alpha = s^a \bmod p$,
und B erhält: $\beta = s^b \bmod p$.
Die Produkte werden öffentlich ausgetauscht. Um das Endprodukt zu erhalten potenzieren die Partner die erhaltenen Werte jeweils mit ihren geheimen Zahlen.
A berechnet: $k = \beta^a \bmod p$,
und B erhält $k` = \alpha^b \bmod p$.
Die beiden Werte $k = s^{ba} \bmod p = s^{ab} \bmod p = k`$ stimmen überein und kein Gegner kann sie berechnen.
Die „diskrete“ Exponentialfunktion $a \to s^a \bmod p$ ist leicht ausführbar, ihre Umkehrung, die diskrete Logarithmusfunktion ist nach heutigem Wissen praktisch unmöglich ausführbar. Sie ist eine Einwegfunktion.

4.4 Public-Key-Verfahren

Jeder Teilnehmer an einem Public-Key-Verfahren hat einen geheimen Schlüssel (pivate key) zum Entschlüsseln an ihn gesendeter Nachrichten. Zu diesem passend gibt es einen öffentlichen Schlüssel (public key) zum Verschlüsseln von Botschaften. Will man jemanden eine geheime Mitteilung senden, verwendet man dessen public key zum Chiffrieren. Aus dessen Kenntnis auf den geheimen zu schließen ist praktisch unmöglich. Diese theoretischen Grundlagen erkannten Diffie und Hellman. Sie fanden aber nicht die praktische Existenz des Verfahrens.
Das Public-Key-Kryptosystem ist genau das Gegenteil der bisher verwendeten Methoden, die alle auf symmetrische Verschlüsselung beruhten. Es wurde mit demselbem Schlüssel ver- und entschlüsselt. Nun handelt es sich um eine asymmetrische Chiffrierung.

4.5 RSA Verfahren

Ron Rivest, Adi Shamir und Leonard Adleman lieferten nach längerer Forschungsarbeit 1977 die praktische Lösung zum Public-Key-Kryptosystem, das nach ihnen benannte RSA-Verfahren.

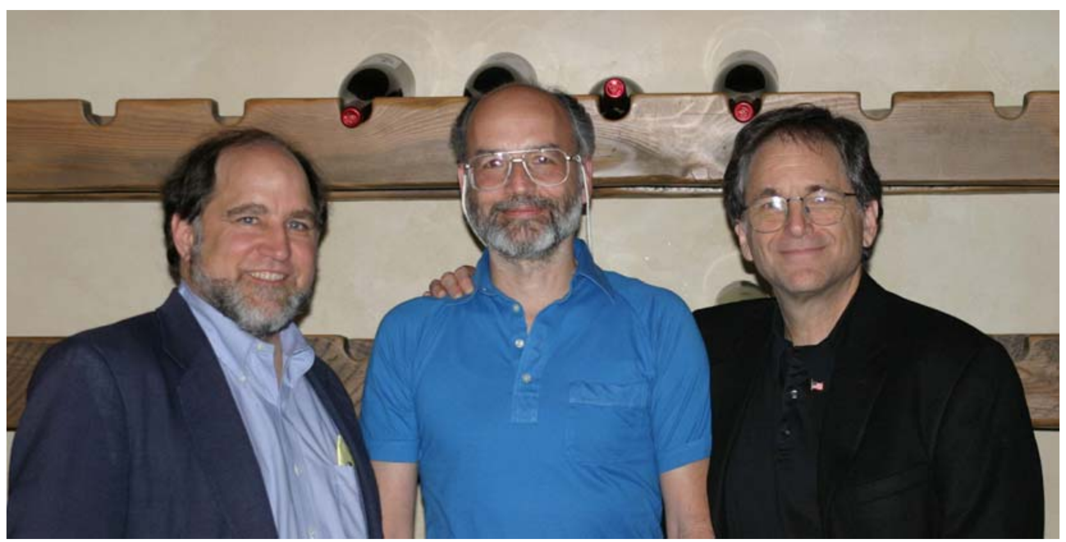


Abb. 17 Ron Rivest, Adi Shamir und Leonard Adleman (2003)

Der Empfänger A wählt zwei hinreichend große Primzahlen p und q, bildet deren Produkt $N = p \times q$. Der public key N wird veröffentlicht und jeder kann mit einem vorher vereinbarten Einwegverfahren seine Botschaft verschlüsseln und an A schicken. Nur A kann durch Kenntnis von p und q das Einwegverfahren umkehren und die ihm gesendeten Botschaften entschlüsseln.
Vorausgesetzt es gibt keine andere Möglichkeit das RSA-Verfahren zu knacken, als die Primzahlzerlegung, ist dies genauso schwierig, wie große Zahlen zu faktorisieren. Bis heute ist keine andere Methode bekannt.
Wollte ein Angreifer aus N die Primfaktoren p und q berechnen, bräuchte er auf Grund der Größe der gewählten Primzahlen (im Bereich von je 10^{154} bei wichtigen Banktransaktionen) nach heutigem Wissen auch mit allen Computern der Welt länger als das Universum alt ist.
RSA hat den großen Nachteil, dass komplizierte, länger Berechnungen nötig sind und war daher anfangs nur für Regierungen, Militär und große Unternehmen einsetzbar.

4.6 PGP

Phil Zimmerman entwickelte das Verfahren „Pretty Good Privacy“ kurz PGP, das das Verschlüsseln von Botschaften ab 1991 auch normalen Menschen ermöglicht. Es setzt sich nur aus bekannten Mechanismen zusammen und wird auf Grund seiner Benutzerfreundlichkeit von Millionen von Personen benutzt.

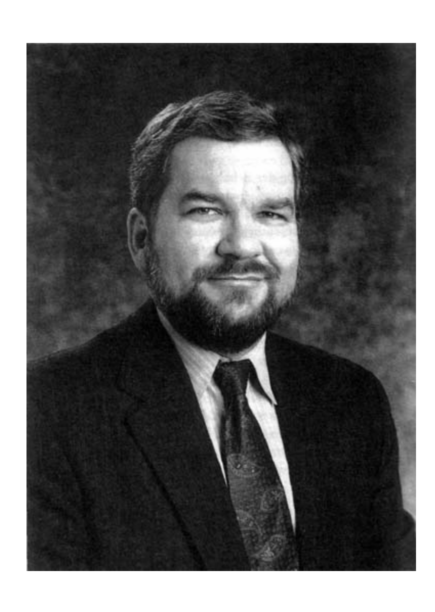


Abb. 18: Phil Zimmerman

Man verwendetet erstens eine symmetrische Verschlüsselung, nämlich IDEA, die ähnlich funktioniert wie DES nur die 64 Bitblöcke mit 128 Bit Schlüsseln chiffriert. Zur Übertragung des IDEA Schlüssels verwendet man zweitens RSA als Public-Key-Verfahren. Somit gewinnt man die Sicherheit und den Schlüsselaustausch des einen Verfahrens und die Schnelligkeit des anderen.
Die Verwendung von PGP ist keineswegs unumstritten, so befürchten Gegner den vermehrten Einsatz durch das organisierte Verbrechen bzw. durch Terroristen. Befürworter sehen darin die einzige Möglichkeit seine Privatsphäre im Informationszeitalter zu schützen.

Resümee

Kryptographie wurde erst in den letzten Jahrzehnten zu einer anerkannten Wissenschaft. Ohne sie sind moderne Kommunikations- und Informationssysteme nicht mehr denkbar. Sie bietet jedem die Möglichkeit seine Privatsphäre zu schützen. Andererseits ermöglicht sie Verbrechern unentdeckt untereinander zu kommunizieren.
Der Kampf zwischen Kryptographen und Kryptoanalytikern wurde über Jahrtausende ausgetragen und wird auch in Zukunft kein Ende haben. Es stellt sich die Frage: Gibt es die unknackbare und auch praktikable Verschlüsselung schlechthin?

Quellenverzeichnis

- Bauer,F.L., *Entzifferte Geheimnisse*, Berlin Heidelberg 1997
- Beutelspacher, Albrecht, *Geheimsprachen. Geschichte und Techniken,* München 1997
- Melton, H.Keith, *Der perfekte Spion*, München
- Singh, Simon, *Geheime Botschaften*, Originaltitel: *The Code Book. The Sience of Secrecy from Ancient Egypt to Quantum Cryptography,* London 1999
- Stix, Franz, *Zur Geschichte und Organisation der Geheimen Wiener Ziffernkanzlei*, Wien

Abbildungsverzeichnis